93D CONGRESS
1ST SESSION

H. R. 10042

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 5, 1973

Mr. GOLDWATER introduced the following bill; which was referred to the Committee on the Judiciary

A BILL

To provide standards of fair personal information practices.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. This Act may be cited as the "Code of Fair Information Practices of 1973".

FINDINGS AND DECLARATION OF PURPOSE

SEC. 2. (a) The Congress finds—

(1) that an individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record;

(2) that a record containing information about an individual in identifiable form must be governed by

procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it;

(3) that any recording, disclosure, and use of identifiable personal information by an organization not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure, or use is specifically authorized by Federal statute.

(b) The purpose of this Act is to insure safeguards for personal privacy from recordkeeping organizations by adherence to the following principles of information practice:

(1) There must be no personal data recordkeeping systems whose very existence is secret.

(2) There must be a way for an individual to find out what information about him is in a record and how it is used.

(3) There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.

(4) There must be a way for an individual to correct or amend a record of identifiable information about him.

(5) Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

(6) Deviations from these principles should be permitted only if it is clear that some significant interest of the individual data subject will be served or if some paramount societal interest can be clearly demonstrated. No deviation should be permitted except as specifically provided by statute.

DEFINITIONS

SEC. 3. For the purposes of this Act—

(a) The term "automated personal data system" means a collection of records containing personal data that can be associated with identifiable individuals, and that are stored, in whole or in part, in computer-accessible files.

(b) The term "data that can be associated with identifiable individuals" means that by some specific identification, such as a name or social security number, or because they include personal characteristics, it is possible to identify an individual with reasonable certainty.

(c) The term "personal data" includes all data that describes anything about an individual, such as identifying characteristics, measurements, test scores; that evidence

things done by or to an individual such as records of financial transactions, medical treatment, or other services; or that afford a clear basis for inferring personal characteristics or things done by or to an individual, such as the mere record of his presence in a place, attendance at a meeting, or admission to some type of service institution.

(d) The term "computer accessible" means recorded on magnetic tape, magnetic disk, magnetic drum, punched card, or optically scannable paper or film.

(e) The term "data system" includes all processing operations, from initial collection of data through all uses of the data, including outputs from the system. Data recorded on questionnaires, or stored in microfilm archives, are considered part of a data system, even when the computer-accessible files themselves do not contain identifying information.

(f) The term "organization" means any Federal agency; the courts of the United States; the government of the District of Columbia; any public or private corporation, partnership, agency, or association which operates an administrative automated personal data system, or a statistical-reporting and research automated personal data system; and which is supported in whole or in part by Federal funds, Federal systems, or federally supported systems, or which directly or indirectly makes use of any means or instruments of transportation or communications in interstate commerce,

or of the mails, or which carries or causes to be carried in the mails or interstate commerce, or by any other means or instruments of transportation any personal data; and any organization which maintains a record of individually identifiable personal data which it does not maintain as part of an administrative or as a statistical-reporting and research automated personal data system and which transfers such data to one of the above organizations in interstate commerce.

(g) The term "administrative personal data system" means one that maintains data on individuals for the purpose of affecting them directly as individuals; and for making determinations relating to their qualifications, character, rights, opportunities, or benefits.

(h) The term "statistical-reporting or research system" means one that maintains data about individuals exclusively for statistical reporting or research and is not intended to be used to affect any individual directly.

(i) The term "unfair personal information practice" means a failure to comply with any safeguard requirements of this Act.

(j) The term "data subject" means the individual whose name or identity is added to or maintained on an automated personal data system or a statistical-reporting or research system.

SAFEGUARD REQUIREMENTS FOR ADMINISTRATIVE PERSONAL DATA SYSTEMS

SEC. 4. (a) GENERAL REQUIREMENTS.—(1) Any organization maintaining a record of individually identifiable personal data, which it does not maintain as part of an administrative automated personal data system, shall make no transfer of any such data to another organization, without the prior informed consent of the individual to whom the data pertain, if, as a consequence of the transfer, such data will become part of an administrative automated personal data system that is not subject to these safeguard requirements.

(2) Any organization maintaining an administrative automated personal data system shall—

(A) identify one person immediately responsible for the system, and make any other organizational arrangements that are necessary to assure continuing attention to the fulfillment of these safeguard requirements;

(B) take affirmative action to inform each of its employees having any responsibility or function in the design, development, operation, or maintenance of the system, or the use of any data contained therein, about all these safeguard requirements and all the rules and procedures of the organization designed to assure com-

pliance with them, and the nature of such action shall be supplied upon the reasonable request of a data subject;

(C) specify penalties to be applied to any employee who initiates or otherwise contributes to any disciplinary or other punitive action against any individual who brings to the attention of appropriate authorities, the press, or any member of the public, evidence of unfair personal information practice;

(D) take reasonable precautions to protect data in the system from any anticipated threats or hazards to the security of the system;

(E) make no transfer of individually identifiable personal data to another system without (i) specifying requirements for security of the data, including limitations on access thereto, and (ii) determining that the conditions of the transfer provide substantial assurance that those requirements and limitations will be observed—except in instances when an individual specifically requests that data about him be transferred to another system or organization;

(F) maintain a complete and accurate record of every access to and use made of any data in the system, including the identity of all persons and organizations to which access has been given;

(G) maintain data in the system with which such accuracy, completeness, timeliness, and pertinence as is necessary to assure accuracy and fairness in any determination relating to an individual's qualifications, character, rights, opportunities, or benefits, that may be made on the basis of such data.

(b) Any organization maintaining an administrative automated personal data system that publicly disseminates statistical reports or research findings based on personal data drawn from the system, or from systems of other organizations, shall—

(1) make such data publicly available for independent analysis, on reasonable terms; and

(2) take reasonable precautions to assure that no data made available for independent analysis will be used in a way that might reasonably be expected to prejudice judgments about any individual data subject's character, qualifications, rights, opportunities, or benefits.

(c) PUBLIC NOTICE REQUIREMENT.—Any organization maintaining an administrative automated personal data system shall give public notice of the existence and character of its system once each year, in the case of Federal organizations in the Federal Register, or in the case of other organizations, in a media likely to bring attention to the evidence of

the records to the data subject. Any organization maintaining more than one system shall publish such annual notices for all its systems simultaneously. Any organization proposing to establish a new system, or to enlarge an existing system, shall give public notice long enough in advance of the initiation or enlargement of the system to assure individuals who may be affected by its operation a reasonable opportunity to comment. The public notice shall specify:

(1) The name of the system.

(2) The nature and purpose (s) of the system.

(3) The categories and number of persons on whom data are (to be) maintained.

(4) The categories of data (to be) maintained, indicating which categories are (to be) stored in computer-accessible files.

(5) The organization's policies and practices regarding data storage, duration of retention of data, and disposal thereof.

(6) The categories of data sources.

(7) A description of all types of use (to be) made of data, indicating those involving computer-accessible files, and including all classes of users and the organizational relationships among them.

(8) The procedures whereby an individual can (A) be informed if he is the subject of data in the systems;

(B) gain access to such data; and (C) contest their accuracy, completeness, timeliness, pertinence, and the necessity for retaining it.

(9) The procedures whereby an individual, group, or organization can gain access to data used for statistical reporting or research in order to subject such data to independent analysis.

(10) The title, name, and address of the person immediately responsible for the system.

(11) A description of the penalties to be applied to any employee who initiates or otherwise contributes to any disciplinary or other punitive action against any individual who brings attention to any evidence of unfair information practices.

(d) RIGHTS OF INDIVIDUAL DATA SUBJECTS.—Any organization maintaining an administrative automated personal data system shall—

(1) inform an individual asked to supply personal data for the system whether he is legally required, or may refuse, to supply the data requested, and also of any specific consequences for him, which are known to the organization, of providing or not providing such data;

(2) upon request and proper identification of any

data subject, clearly and accurately disclose to the data subject, in a form comprehensible to him—

(A) all data about the data subject;

(B) the sources of the information;

(C) the recipients of any transfer, report, dissemination, or use of data about the data subject, including the identity of all persons and organizations involved and their relationship to the system;

(3) comply with the following minimum conditions of disclosure to data subjects—

(A) an organization shall make the disclosures required under subsection 4(d) (2) during normal business hours;

(B) the disclosures required under section 4 (d) (2) shall be made to the data subject (i) in person if he appears in person and furnishes proper identification; the data subject is entitled to personal, visual inspection of data about him; or (ii) by telephone if he has made a written request, with proper identification; telephone disclosures are to be made without charge to the data subject; and (iii) by mail if he has made a written request, with proper identification; and (iv) by providing a copy of his file, if

requested, at a charge not to exceed 10 cents per page;

(C) the data subject shall be permitted to be accompanied by one person of his choosing, who shall furnish reasonable identification. An organization may require the data subject to furnish a written statement granting permission to the organization to discuss the data subject's file in such person's presence;

(D) subsection 4(d)(2) disclosure, shall not apply to subject files that are (i) directly related to international relations or international subversive activities, or (ii) active criminal investigatory data, except active criminal investigatory data which has been maintained for a period longer than reasonably necessary to bring indictment, information, or to commence prosecution.

(4) assure that no use of individually identifiable data is made that is not within the stated purposes of the system as reasonably understood by the individual, unless, in the case of each use of such data, the informed consent of the individual has been obtained in writing;

(5) assure that no data about an individual is made available from the system in response to a demand for data made by means of compulsory legal process, unless

the individual to whom the data pertain has been notified of the demand; and

(6) if the completeness, accuracy, pertinence, timeliness, or necessity for retaining the data in the system is disputed by the data subject and the dispute is directly conveyed to the organization by the data subject, the following minimum procedures shall be followed:

(A) The organization shall within a reasonable period of time investigate and record the current status of that data unless it has reasonable grounds to believe that the dispute by the data subject is frivolous or irrelevant.

(B) If, after such investigation, such data is found to be inaccurate or can no longer be verified, the organization shall promptly delete such data.

(C) The presence of contradictory information in the data subject's file does not in and of itself constitute reasonable grounds for believing the dispute is frivolous or irrelevant.

(D) If the investigation does not resolve the dispute, the data subject may file a brief statement setting forth the nature of the dispute; the organization may limit such statements to not more than one hundred words if the organization provides the

data subject with assistance in writing a clear summary of the dispute.

(E) Whenever a statement of a dispute is filed, unless there are reasonable grounds to believe that it is frivolous or irrelevant, the organization shall, in any subsequent transfer, report, or dissemination of the data in question, clearly note that it is disputed by the data subject and provide either the data subject's statement or a clear and accurate summary thereof.

(F) Following any deletion of data which is found to be inaccurate or whose accuracy can no longer be verified or any notation as to disputed data, the organization shall, at the request of the data subject, furnish notification that the item has been deleted, or a statement, or summary, which contains the deleted or disputed information to any person specifically designated by the data subject.

(i) The organization shall clearly and conspicuously disclose to the data subject his rights to make such a request.

SAFEGUARD REQUIREMENTS FOR STATISTICAL-REPORTING AND RESEARCH SYSTEMS

SEC. 5. (a) GENERAL REQUIREMENTS.—(1) Any organization maintaining a record of personal data, which it does not maintain as part of an automated personal data

system used exclusively for statistical-reporting or research, shall make no transfer of any such data to another organization without prior informed consent of the individual to whom the data pertain, if, as a consequence of the transfer, such data will become part of an automated personal data system that is not subject to these safeguard requirements or the safeguard requirements for administrative personal data systems.

(2) Any organization maintaining an automated personal data system used exclusively for statistical-reporting or research shall—

(A) identify one person immediately responsible for the system, and make any other organizational arrangements that are necessary to assure continuing attention to the fulfillment of the safeguard requirements;

(B) take affirmative action to inform each of its employees having any responsibility or function in the design, development, operation, or maintenance of the system, or the use of any data contained therein, about all the safeguard requirements and all the rules and procedures of the organization designed to assure compliance with them;

(C) specify penalties to be applied to any employee who initiates or otherwise contributes to any disciplinary or other punitive action against any individual who

brings to the attention of appropriate authorities, the press, or any member of the public, evidence of unfair personal information practice;

(D) take reasonable precautions to protect data in the system from any anticipated threats or hazards to the security of the system;

(E) make no transfer of individually identifiable personal data to another system without (i) specifying requirements for security of the data, including limitations on access thereto, and (ii) determining that the conditions of the transfer provide substantial assurance that those requirements and limitations will be observed—except in instances when each of the individuals about whom data is to be transferred has given his prior informed consent to the transfer; and

(F) have the capacity to make fully documented data readily available for independent analysis.

(b) PUBLIC NOTICE REQUIREMENT.—Any organization maintaining an automated personal data system used exclusively for statistical-reporting or research shall give public notice of the existence and character of its system once each year, in the case of Federal organizations in the Federal Register, or in the case of other organizations, in a media likely to bring attention to the existence of the records to the data subject. Any organization maintaining more

than one such system shall publish annual notices for all its systems simultaneously. Any organization proposing to establish a new system, or to enlarge an existing system, shall give public notice long enough in advance of the initiation or enlargement of the system to assure individuals who may be affected by its operation a reasonable opportunity to comment. The public notice shall specify—

(1) the name of the system;

(2) the nature and purpose (s) of the system;

(3) the categories and number of persons on whom data are (to be) maintained;

(4) the categories of data (to be) maintained, indicating which categories are (to be) stored in computer-accessible files;

(5) the organization's policies and practices regarding data storage, duration of retention of data, and disposal thereof;

(6) the categories of data sources;

(7) a description of all types of use (to be) made of data, indicating those involving computer-accessible files, and including all classes of users and the organizational relationships among them;

(8) the procedures whereby an individual, group, or organization can gain access to data for independent analysis;

(9) the title, name, and address of the person immediately responsible for the system;

(10) a statement of the system's provisions for data confidentiality and the legal basis for them.

(c) RIGHTS OF INDIVIDUAL DATA SUBJECTS.—Any organization maintaining an automated personal data system used exclusively for statistical-reporting or research shall—

(1) inform an individual asked to supply personal data for the system whether he is legally required, or may refuse, to supply the data requested, and also of any specific consequences for him, which are known to the organization, of providing or not providing such data;

(2) assure that no use of individually identifiable data is made that is not within the stated purposes of the system as reasonably understood by the individual, unless, in the case of each use of such data, the informed consent of the individual has been explicitly obtained;

(3) assure that no data about an individual and made available from the system in response to a demand for data made by means of compulsory legal process, unless the individual to whom the data pertain—

(A) has been notified of the demand, and

(B) has been afforded full access to the data before they are made available in response to the demand.

ENFORCEMENT

SEC. 6. (a) INJUNCTIONS FOR COMPLIANCE.—Whenever it appears to the Attorney General of the United States that any organization has engaged, is engaged, or is about to engage in any acts or practices constituting an unfair personal information practice under this Code, he may by his own discretion bring an action, in the district court of the United States or the appropriate United States court of any territory or other place subject to the jurisdiction of the United States, to enjoin such acts or practices, and showing there is or is about to be such engagement, a permanent or temporary injunction or restraining order shall be granted without bond. Upon application of the Attorney General any such court may also issue injunctions commanding any organization to comply with any section of the Code. The court may grant as relief, as it deems appropriate, any permanent, or temporary injunction, temporary restraining order, or other order, at the prayer of a data subject or class of data subjects.

(b) CIVIL LIABILITY FOR UNFAIR PERSONAL INFORMATION PRACTICE.—Any organization which commits an unfair personal information practice shall be liable in an amount equal to the sum of—

(1) any actual damages sustained by the data sub-

ject (s) as a result of the unfair practice, but not less than liquidated damages of $10,000; and

(2) such amount of punitive damages as the court may allow; and

(3) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

(c) CRIMINAL LIABILITY FOR UNFAIR PERSONAL INFORMATION PRACTICES BY FEDERAL OFFICERS OF EMPLOYEES.—Any officer or employee of any Federal agency, the courts of the United States, the governments of the territories or possessions of the United States, or the government of the District of Columbia who willingly or knowingly permits or causes to occur an unfair personal information practice shall be fined not more than $10,000 or imprisoned not more than one year or, suspended from employment without pay for not more than one year, or all three.

(d) JURISDICTION OF COURTS; LIMITATIONS OF ACTIONS.—An action to enforce any liability created under this Code may be brought in any appropriate United States district court without regard to the amount in controversy, or in any other court or competent jurisdiction, within two years from the date on which the liability arises, except where a defendant has materially and willfully failed to com-

ply with the safeguards under this Code, the action may be brought at any time within two years after discovery by the individual data subject.

SEVERABILITY

SEC. 7. If any provision of this Code or the application thereof to any particular circumstance or situation is held invalid, the remainder of this Code, or the application of such provision to any other circumstance or situation shall not be affected thereby.

EFFECTIVE DATE

SEC. 8. This Code shall take effect one year after the date of its enactment.

STATE LAWS

SEC. 9. (a) No State law in effect on the date of passage of this Act or which may become effective thereafter shall be superseded by any provision of this Code except insofar as such State law is in conflict with this Code.

(b) The provisions of any State law or regulation in effect upon the effective date of this Act, or which may become effective thereafter, which provide for more stringent safeguard standards than do the provisions of this Code shall not thereby be construed or held to be in conflict with this Code. The provisions of any State law or regulation in effect upon the operative date of this Act, or which become effective thereafter, which provide for safeguard standards for

which no provision is contained in this Code shall not be held to be in conflict with this Code.

FEDERAL AGENCY REGULATIONS

SEC. 10. (a) Each Federal agency shall, with the advice of the Attorney General of the United States pursuant to the Administrative Procedure Act, promulgate, adopt, and from time to time amend and administer comprehensive rules and regulations necessary to further the purposes of this Act for the internal activities of such agency and in a manner consistent with the safeguards specified herein.

(b) Notwithstanding any statute or regulation to the contrary, rules and regulations issued hereunder shall govern and control the collection, security, and dissemination of all automated personal data by each Federal agency.

93D CONGRESS
1ST SESSION

H. R. 10042

A BILL

To provide standards of fair personal information practices.

By Mr. GOLDWATER

SEPTEMBER 5, 1973
Referred to the Committee on the Judiciary

Approved For Release 2002/05/01 : CIA-RDP82-00357R000700120015-0